IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Jing Xiang et al.	§	Art Unit:	2139
		§		
Serial No.:	10/791,414	§		
		§	Examiner:	Amare F. Tabor
Filed:	March 3, 2004	§		
		§		
For:	Technique for Maintaining	§	Atty. Dkt. No.:	NRT.0124US
	Secure Network Connections	§		(16483BAUS01U)
		§		
		§		
		§		

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF PURSUANT TO 37 C.F.R § 41.37

Sir:

The final rejection of claims 1-7, 9-12, 14, 17, and 20-22 is hereby appealed.

I.   REAL PARTY IN INTEREST

The real party in interest is Nortel Networks Limited.

II.   RELATED APPEALS AND INTERFERENCES

None.

III.   STATUS OF THE CLAIMS

Claims 1-7, 9-12, 14, 17, and 20-22 have been finally rejected and are the subject of this appeal. Claims 8, 13, 15, 16, 18, and 19 are cancelled.

IV. STATUS OF AMENDMENTS

No amendment after Final Rejection was filed.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

Independent claim 1 recites a method for maintaining secure network connections, the method comprising:

> detecting (Fig. 2:202) a change of address from an old address to a new address associated with a first network element (Spec., p. 11, lines 3-9);

> updating (Fig. 2:204) at least one first security configuration at the first network element (Spec., p. 11, lines 10-11);

> transmitting (Fig. 2:206) at least one secure message from the first network element to a second network element, wherein the at least one secure message contains both the old address and the new address (Spec., p. 11, lines 12-16),

> wherein the old address and the new address in the at least one secure message enables at least one second security configuration at the second network element to be updated (Spec., p. 11, line 22-p. 12, line 10).

Independent claim 10 recites a method for maintaining secure network connections, the

method comprising:

duplicating, at a third network element (Fig. 5:504), information associated with a secure network connection between a first network element (Fig. 5:500) and a second network element (Fig. 5:502), wherein a lookup of security associations associated with the secure network connection is not dependent on any destination address (Spec., p. 9, lines 21-22; p. 10, lines 15-17; p. 14, lines 16-21); and

in response to detecting failure of the second network element, replacing the second network element with the third network element in the secure network connection with the first network element (Spec., p. 14, line 21-p. 15, line 10).

Independent claim 12 recites a method for maintaining secure network connections, the

method comprising:

configuring a plurality of security gateways (Fig. 5:502, 504) such that a lookup of security associations is not dependent on any destination address (Spec., p. 9, lines 21-22; p. 10, lines 15-17); and

sharing at least one security association among the plurality of security gateways (Spec., p. 10, lines 21-23).

Independent claim 22 recites a first security server (Fig. 5:504) comprising:

a transceiver to receive information relating to at least one security association of a secure network connection between a mobile client (Fig. 5:500) and a second security server (Fig. 5:502; Spec., p. 14, lines 15-21); and

a processor module to:

monitor operation of the second security server (Spec., p. 14, lines 21-22);

in response to detecting failure of the second security server, send a message to the mobile client that the first security server is taking over the secure network connection (Spec., p. 14, line 22-p. 15, line 2); and

communicate with the mobile client using the at least one security association over the secure network connection between the first security server and the mobile client (Spec., p. 15, lines 4-10).

3

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A.   **Claims 1-7, 9, 10, 20, and 21 Rejected Under 35 U.S.C. § 102(b) as Anticipated by U.S. Patent No. 6,976,177 (Ahonen).**

B.   **Claims 11, 12, 14, 17, and 22 Rejected Under 35 U.S.C. § 103(a) as Unpatentable Over Ahonen in View of U.S. Patent Application Publication No. 2004/0117653 (Shapira).**

VII.   ARGUMENT

The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-headings as required by 37 C.F.R. § 41.37(c)(1)(vii).

A.   **Claims 1-7, 9, 10, 20, and 21 Rejected Under 35 U.S.C. § 102(b) as Anticipated by U.S. Patent No. 6,976,177 (Ahonen).**

1.   Claims 10, 20, 21.

Independent claim 10 was erroneously rejected as being anticipated by Ahonen.

Claim 10 recites a method for maintaining secure network connections that comprises:

- duplicating, at a third network element, information associated with a secure network connection between a first network element and a second network element, wherein a lookup of security associations associated with the secure network connection is not dependent on any destination address; and

- **in response to detecting failure** of the second network element, **replacing** the second network element with the third network element in the secure network connection with the first network element.

Ahonen fails to disclose at least the "replacing" element of claim 10, in combination with the "duplicating" element of claim 10.

As disclosing the "replacing" element of claim 10, the Examiner cited the following passages of Ahonen: ¶¶ [0004]-[0015]; Figs. 2-3; ¶¶ [0047], [0088]; ¶¶ [0108], [0146]-[0156].

None of these passages even remotely hint at detecting **failure** of the second network element.

Paragraphs [0004]-[0015] of Ahonen refer to a mobile host communicating with a correspondent host over a VPN via a security gateway, in which the mobile host and correspondent host negotiate a security association. Subsequently a communication between the mobile host and security gateway is established, and an authentication certificate is sent to the security gateway. Next, data packets are sent from the mobile host to the correspondent host using the identified security association, via the security gateway. The cited passages also refer to negotiating one or more security associations between the mobile host and the security gateway. The cited passages also refer to the fact that a virtual private network may comprise an intranet, with the security gateway being coupled between the intranet and the Internet. The cited passages also note that the correspondent host may reside within the intranet, or may reside outside of the intranet.

Nowhere in these passages of Ahonen is there any remote hint of **detecting failure** of the second network element, as recited in claim 10. On page 4 of the Office Action, the Examiner stated that "communication between mobile and correspondent hosts through the security gateway/firewall 3 is disclosed as 'preferable'." However, this has nothing to do with detecting failure of a second network element, and replacing the second network element in the secure network connection with the third network element in response to detecting the failure.

Figs. 2 and 3 of Ahonen also do not provide any teaching of detecting failure of a second network element, and replacing the second network element with a third network element in the secure network connection with the first network element in response to detecting the failure.

Paragraph [0047] of Ahonen refers to a preparations function (Phase 1), in which a single ISAKMP security association is negotiated between the mobile host and the firewall. Paragraph [0088] of Ahonen refers to Phase 2, in which security associations are negotiated between the mobile host and the firewall, and between the mobile host and the correspondent host. Again, absolutely no reference is made to detecting failure of a second network element, and replacing the second network element with a third network element as recited in claim 10.

Paragraph [0108] of Ahonen refers to a remote control function that is used by the mobile host to remotely activate preexisting secure connections to the correspondent host. There is no mention of detecting failure of a second network element, and replacing the second network element with a third network element as recited in claim 10.

The passages in paragraphs [0146]-[0156] also provide absolutely no hint whatsoever of detecting failure of a second network element, and replacing the second network element with a third network element in the secure network connection with the first network element in response to detecting the failure of the second network element.

In view of the foregoing, it is clear that claim 10 and its dependent claims are not anticipated by Ahonen.

Reversal of the final rejection of the above claims is respectfully requested.

2. Claims 1-7, 9.

Independent claim 1 was also erroneously rejected as being anticipated by Ahonen.

Claim 1 recites a method for maintaining secure network connections that comprises:

- detecting a change of address from an old address to a new address associated with a first network element;

- updating at least one first security configuration at the first network element;

- transmitting at least one secure message from the first network element to a second network element, wherein the at least one secure message contains both the old address and the new address,

- wherein the old address and the new address in the at least one secure message enables at least one second security configuration at the second network element to be updated.

According to claim 1, at least one secure message is transmitted from the first network element to a second network element, where the at least one secure message contains both the old address and the new address associated with the first network element (due to a change of address). The Examiner cited the following passages of Ahonen as disclosing this claim feature: ¶¶ [0097]-[0105] and [0111]-[0118]. The passages beginning at ¶ [0097] of Ahonen refer to the mobile host sending an authorization certificate to a firewall, where the certificate includes a list of identities of Phase 2 security associations that were pre-created. The information about each security association includes the source and destination IP addresses. However, such source and destination IP addresses do not constitute the old address and new address associated with the first network element (due to a change of address) that is contained in the secure message of claim 1.

The passages beginning in ¶ [0111] of Ahonen refer to the mobile host sending a control authorization certificate to the firewall, where the control authorization certificate contains new source and destination IP addresses. However, this control authorization certificate would only include the new addresses, and would not include both the old and new addresses associated with the first network element. Therefore, it is clear that nothing in Ahonen even remotely hints at a secure message that contains both the old address and new address.

In view of the foregoing, it is respectfully submitted that claim 1 and its dependent claims are not anticipated by Ahonen.

Reversal of the final rejection of the above claims is respectfully requested.

B.   Claims 11, 12, 14, 17, and 22 Rejected Under 35 U.S.C. § 103(a) as Unpatentable Over Ahonen in View of U.S. Patent Application Publication No. 2004/0117653 (Shapira).

1.   Claims 14, 17, 22.

The Examiner erroneously rejected independent claim 22 as being obvious over Ahonen and Shapira.

To make a determination under 35 U.S.C. § 103, several basic factual inquiries must be performed, including determining the scope and content of the prior art, and ascertaining the differences between the prior art and the claims at issue. *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 U.S.P.Q. 459 (1965). Moreover, as a recent U.S. Supreme Court held, it is important to identify a reason that would have prompted a person of ordinary skill in the art to combine reference teachings in the manner that the claimed invention does. *KSR International Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1741, 82 U.S.P.Q.2d 1385 (2007).

With respect to claim 22, the Examiner conceded that Ahonen fails to disclose a processor module in a first security server to monitor operation of a second security server. 1/22/2008 Office Action at 7. However, the Examiner relied upon Shapira as purportedly disclosing this claim feature missing from Ahonen. *Id.*

The processor module of claim 22 performs the following tasks:

* monitor operation of the second security server;

* in response to detecting failure of the second security server, send a message to the mobile client that the first security server is taking over the secure network connection; and

* communicate with the mobile client using the at least one security association over the secure network connection between the first security server and the mobile client.

The Examiner is incorrect in asserting that Shapira discloses claim features that are missing from Ahonen. Neither Ahonen nor Shapira even remotely hints at the processor module of a first security server to monitor operation of a second security server, and in response to detecting failure of the second security server, and send a message to the mobile client that the first security server is taking over the secure network connection.

The Examiner cited the security processor 88 in Fig. 3 of Shapira as being the processor module of claim 22. *Id.* at 7. This security processor 88 of Shapira is a VPN security processor that has a plurality of security engines 90 "each adapted and configured to perform a particular security related operation," such as "encryption, decryption, authentication, the DES algorithm, Header Message Authentication Code (HMAC), etc." Shapira, ¶ [0057]. There is absolutely nothing in Shapira to teach that the processor module is able to perform the tasks recited in claim 22.

Therefore, even if Ahonen and Shapira could be hypothetically combined, the hypothetical combination would not have led to the claimed invention.

Moreover, it is respectfully submitted that a person of ordinary skill in the art would not have been prompted to combine the teachings of Ahonen and Shapira to achieve the claimed invention. The cited references make absolutely no reference whatsoever to detecting failure and one security server taking over a secure network connection with a mobile client in place of another security server. Therefore, a person of ordinary skill in the art reading the teachings of the references would not have been led to the claimed invention.

In view of the foregoing, it is clear that the obviousness rejection of claim 22 and its dependent claims is defective.

Reversal of the final rejection of the above claims is respectfully requested.

2.   **Claim 12.**

Independent claim 12 was rejected as being obvious over Ahonen and Shapira. With respect to claim 12, the Examiner conceded that Ahonen fails to disclose a plurality of security gateways and sharing at least one security association among the plurality of security gateways. 1/22/2008 Office Action at 6. However, the Examiner relied upon Shapira as disclosing the claim feature missing from Ahonen.

With respect to Shapira, the Examiner cited Fig. 1 of Shapira as disclosing the plurality of security gateways. Fig. 1 shows a PDA 12, a cable plug adapter 18, and a computer 28, each including a corresponding VPN mechanism 14, 20, and 30. However, there is no indication that the VPN mechanisms 14, 20, and 30 actually share any security association. Therefore, even if Ahonen and Shapira could be hypothetically combined, the hypothetical combination would not have led to the claimed subject matter.

In view of the foregoing, it is respectfully submitted that the obviousness rejection of claim 12 is defective.

Reversal of the final rejection of the above claim is respectfully requested.

3.   **Claim 11.**

Claim 11 depends from claim 10. In view of the fact that claim 10 is allowable over Ahonen, it is respectfully submitted that the obviousness rejection of claim 11 over Ahonen and Shapira is also defective. Moreover, claim 11 recites sending at least one secure message from the third network element to the first network element to notify that the first network element that the secure network connection would be taken over by the third network element, where taking over such secure network connection is in response to detecting failure of the second network element. As noted above, the hypothetical combination of Ahonen and Shapira would

not have led to this claimed subject matter. Moreover, no reason existed that would have

prompted a person of ordinary skill in the art to combine the teachings of Ahonen and Shapira.

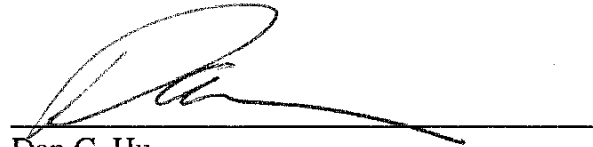Therefore, the obviousness rejection of claim 11 is defective.

Reversal of the final rejection of the above claim is respectfully requested.

CONCLUSION

In view of the foregoing, reversal of all final rejections and allowance of all pending

claims is respectfully requested.

Respectfully submitted,

Date: $5-27-2008$

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

VIII. APPENDIX OF APPEALED CLAIMS

The claims on appeal are:

1 1.   A method for maintaining secure network connections, the method comprising:

2   detecting a change of address from an old address to a new address associated with a first

3 network element;

4   updating at least one first security configuration at the first network element;

5   transmitting at least one secure message from the first network element to a second

6 network element, wherein the at least one secure message contains both the old address and the

7 new address,

8   wherein the old address and the new address in the at least one secure message enables at

9 least one second security configuration at the second network element to be updated.

1 2.   The method according to claim 1, wherein a lookup of security associations is not

2 dependent on any destination address.

1 3.   The method according to claim 1, wherein the first network element is a mobile client

2 and the second network element is a security gateway.

1 4.   The method according to claim 1, wherein the first network element and the second

2 network element are part of a virtual private network (VPN).

1 5.   The method according to claim 1, wherein communications between the first network

2 element and the second network element are based on a security architecture for the internet

3 protocol (IPsec).

1 6.   The method according to claim 5, wherein at least part of the communications between

2 the first network element and the second network element are based on an internet security

3 association and key management protocol (ISAKMP).

1   7.   The method according to claim 6, further comprising the second network element

2   identifying at least one security association based on at least one cookie field in the at least one

3   secure message.

1   9.   At least one processor readable medium for storing a computer program of instructions

2   configured to be readable by at least one processor for instructing the at least one processor to

3   execute a computer process for performing the method as recited in claim 1.

1   10.   A method for maintaining secure network connections, the method comprising:

2   duplicating, at a third network element, information associated with a secure network

3   connection between a first network element and a second network element, wherein a lookup of

4   security associations associated with the secure network connection is not dependent on any

5   destination address; and

6   in response to detecting failure of the second network element, replacing the second

7   network element with the third network element in the secure network connection with the first

8   network element.

1   11.   The method according to claim 10 further comprising sending at least one secure

2   message from the third network element to the first network element to notify the first network

3   element that the secure network connection will be taken over by the third network element.

1   12.   A method for maintaining secure network connections, the method comprising:

2   configuring a plurality of security gateways such that a lookup of security associations is

3   not dependent on any destination address; and

4   sharing at least one security association among the plurality of security gateways.

1   14.   The first security server according to claim 22, wherein a lookup of security associations

2   is not dependent on any destination address.

1   17.   The first security server according to claim 22, wherein communications between the

2   mobile client and the first security server are based on a security architecture for the internet

3   protocol (IPsec).

1   20.   The method of claim 10, further comprising:

2   during life of the secure network connection between the first and second network

3   elements, the third network element receiving information relating to one or more security

4   associations of the secure network connection from the second network element.

1   21.   The method of claim 20, wherein the first network element is a mobile client, and the

2   second and third network elements are security servers.

1   22.   A first security server comprising:

2   a transceiver to receive information relating to at least one security association of a secure

3   network connection between a mobile client and a second security server; and

4   a processor module to:

5   monitor operation of the second security server;

6   in response to detecting failure of the second security server, send a message to

7   the mobile client that the first security server is taking over the secure network connection; and

8   communicate with the mobile client using the at least one security association

9   over the secure network connection between the first security server and the mobile client.

IX.   EVIDENCE APPENDIX

None.

X.   RELATED PROCEEDINGS APPENDIX

None.